# Audit of Security Function
# Report on Preliminary Phase

**Audit and Evaluation Branch**

**January 2000**

Canada

104-02953/

# TABLE OF CONTENTS


**1.0 Audit Objectives** ..... **1**

**2.0 Audit Scope and Approach** ..... **1**

**3.0 Security Function Management Framework** ..... **1**

3.1 Security Organization ..... 1

3.2 Security Plan and Policy ..... 3

3.3 Cost Recovery for Security Services ..... 4

**4.0 Effectiveness and Efficiency of Security Function Delivery within the Department . 5**

4.1 Security Function Administration ..... 5

4.1.1 Education and Training on Security ..... 5

4.1.2 Classification and Designation of Sensitive Information and Assets ..... 6

4.1.3 Threat and Risk Management Method ..... 6

4.1.4 Offense, Infringement and Other Security-Related Incidents ..... 7

4.2 Physical Security ..... 8

4.2.1 Site and Accommodation of Facilities Enabling Risk Reduction or Elimination ..... 8

4.2.2 Physical Protection Measures ..... 8

4.3 Personnel Security ..... 9

4.4 Security and Management of Emergencies ..... 10

**5.0 Conclusion** ..... **11**

## 1.0 Audit Objectives

The purpose of the preliminary phase of this audit was to evaluate the efficiency of Industry Canada's security function and to identify key aspects of this function which should be subject to a further audit.

The objectives of the preliminary phase were to:

- Evaluate the management framework used by the Security Services Division (SSD), including the efficiency of the departmental security policy and its level of compliance with Treasury Board's security policy; and
- Evaluate the effectiveness and efficiency of security function delivery within the Department.

## 2.0 Audit Scope and Approach

The preliminary phase covered all the departmental sectors, including a summary assessment of security function in the Pacific/Yukon, Quebec and Atlantic Regions through telephone interviews. The following elements were audited:

- Security organization;
- Security administration;
- Physical security;
- Personnel security;
- Emergency security and management; and
- Contract security and management.

The information technology security component, which is now part of the Chief Information Office, was excluded from this audit due to its distinct nature. However, the functional relationships between the informatics security officer and the SSD was assessed.

A total of 15 interviews were conducted with managers and employees related to the security function. Treasury Board's Guide to the Audit of a Security Function (July 1996) was used as a reference tool during the interviews and the review of appropriate documentation.

# 3.0 Security Function Management Framework

## 3.1 Security Organization

All managers are responsible of ensuring security within the Department, whereas the Security Services Division is responsible for the management of the various security function elements.

The Security Services Division (SSD) reports to the Director, Compensation, Security and Management Services of the Human Resources Branch. The Director has seven full-time employees, as well as 27 employees under contract with the Corps of Commissionaires and one with Pinkerton.

The Director of SSD acts as the Departmental Security Officer (DSO), whose mandate is to develop, implement, maintain, coordinate and control Industry Canada's security program. For security matters, departmental sectors report directly to the DSO with the exception of the Canadian Research Council (CRC), the Canadian Intellectual Property Office (CIPO) and Measurement Canada. In these cases the DSO assumes a functional reporting role.

The DSO is assisted by three managers: one for personnel security, one for physical security and contingency planning, and one for cost recovery management and security awareness. Since October 1999, the security function related to information technology falls under the responsibility of the Chief Information Office. According to the manager responsible for this function, the transfer has not led to any negative changes for the SSD, as he must keep the DSO informed of all important information concerning information security. The Human Resources Branch is about to revise the work description for the DSO as a result of this transfer.

The DSO plays a functional reporting role with regard to regions. In all regional offices, officers have been appointed for personnel security, as well as physical security and contingency planning. The latter are responsible for applying adequate security measures, but must share the time assigned to security with other administrative tasks.

During the preliminary phase of this audit, the SSD told auditors that the position of the agent responsible for the electronic integrated system of access control and the identification system is presently occupied by a contract employee. However this position is in process of being staffed. Staffing of this position will help to ensure the continuity of this service.

The audit team also discovered that most of the security function elements are covered by SSD positions. However, the following weaknesses were identified in the security organisation within the Department:

- The SSD provides services to external organizations, among which the most important ones are Citizenship and Immigration Canada (CIC) and the Office of the General Auditor. (This is explained, in part, by the Department's acquisition of the control centre located at the Jean Edmond building where these external organizations are located). However it is

difficult to understand the rationale for this situation, since a higher level of security for the operations of CIC is needed, and that the Department is not the main tenant of the building.

- Some regional officers were not able to state accurately their role and their task definition with regards to security. The DSO argued that the lack of personnel and capital explains why the Division is not fully involved in the regions, particularly for the follow-up of security measures.

On the other hand, the SSD seems to maintain close links with functions related to health and safety at work, property and equipment management, and staffing. External links with organizations such as RCMP (physical security) and PWGSC (contract security), appeared to be satisfactory.

**Recommendation**

It is recommended that the Director, Compensation, Security and Management Services, evaluate the relevancy of providing security (and other) services to other government organizations. This assessment could include a comparative analysis of common security services for other government buildings occupied by different departments.

## 3.2 Security Plan and Policy

Through our preliminary assessment, we found that the Department does not have a formal security plan in place. Although several future initiatives were presented by the SSD staff, they do not seem to be part of a comprehensive plan with short, medium and long-term goals and objectives. Moreover, regional security operations are excluded. This plan should also be integrated in the departmental strategic plan and approved by the senior management. The DSO indicated that efforts are being made to convince senior management to establish a department-wide security plan.

The interviews with security officers in regional offices revealed that some regions do not have a planning process or a program for security. While the Pacific/Yukon Region seems to be more proactive in the application of various measures and in the overall security management for their offices, the Atlantic and Quebec Regions have a rather reactive approach.

It was also noted that the Department does not have an overall security policy. There are some old policies derived from the departments that were part of the amalgamation leading to the creation of Industry Canada. These policies are available on the Intranet site of the Human Resources Branch. However, these policies must be revised to remove any references to the old departments and to reflect the 1994 revised security policy of the government. There does not seem to be any formal agenda for the revision of these policies or the development of a department-wide security policy.

**Recommendations**

The Director, Compensation, Security and Management Services should develop a complete security program, that is a plan which includes all the elements of the security function in all departmental sectors and regions.

The Director, Compensation, Security and Management Services should develop and implement a plan to create a department-wide security policy or to update existing policies.

## 3.3 Cost Recovery for Security Services

The SSD Management Director is responsible for the cost recovery of security services. The Administration Officer, Administrative Services, Human Resources Branch (HRB) does the invoicing and the fund recovery.

There are two types of cost recovery: 1) services offered for other government departments and agencies, and 2) services offered within the Department.

**Services offered for other government departments and agencies**

Presently the Department has service agreements with five organizations: the Millennium Bureau of Canada; Citizenship and Immigration Canada; the Canadian Intellectual Property Office; the Canada Industrial Relations Board; and the Public Service Staff Relations Board. These agreements vary from one to three years with an automatic renewal clause. The agreements are relatively different from each other. Coverage of service levels vary from one part of the security function to the overall corporate services. As well, the recovery terms vary from one agreement to the other (e.g., from a rate per service (ID card, access, etc.) to cost-sharing (Corps of Commissionaires)).

The Administration Agent, Administrative Services, HRB, issues invoices on a quarterly basis.

Auditors also observed that the Department provides services to other organizations without any formal agreement, including the Office of the Auditor General of Canada (ID cards, information desk, basic building service); Human Resources Development Canada (emergency system); and the Canadian Space Agency (emergency system).

Preliminary analysis revealed that the basis used for invoicing is not appropriate. No cost analysis has been carried to determine the actual and absorbed costs for service rates and cost-sharing. Costs are presently based on estimates and no annual analysis is conducted to increment costs depending on the increase of incurred expenses. Moreover, it was noted that the cost-sharing for commissionaires does not include overhead costs (supervision, etc.).

**Services within the Department**

Since 1995, the same services are offered within the Department on a cost-recovery basis. This approach has been implemented to meet a resource shortage within the HRB. The SSD has presently has a $337,000 budget for salaries and $66,000 for operating expenses. It also receives a

budgetary transfer of $400,000 from the Deputy Minister's Office for the Corps of Commissionaires. Through cost-recovery, the SSD has a surplus of approximately $1.2 M.

The cost-recovery operation presents some problems for the organization. First, as security within the Department is a critical function, the SSD and HRB staff indicated that the maintenance of an invoicing system adds work. Moreover, it was noted that:

- The invoicing for each ID card and each access modification request application discourages responsibility centres from requesting the service and creates a situation where longer and more risky periods are requested for the sole purpose of minimizing costs;
- According to the interviews, it is likely that some managers refrain from conducting security audits on temporary employees and consultants in order to avoid the associated costs; and
- The invoicing of SSD staff time leads to the transfer of responsibility centres' operating expenses to cover SSD salary expenses. These transfers between operating expenses and salary distort expenditure report within the Department.

In conclusion, cost-recovery is required for services provided to the other organizations external to the Department. However, it is crucial to have an adequate system which reflects actual and absorbed costs. With regard to internal recovery, this does not seem to be a method any more complicated than a simple budget transfer between responsibility centres.

**Recommendations**

The Director, Compensation, Security and Management Services should develop a system to evaluate actual costs related to SSD operations and should revise these rates on an annual basis.

The Director, Compensation, Security and Management Services should review the internal invoicing policy and use the information derived from the assessment of real costs to establish, at the beginning of each year, a budgetary transfer from other responsibility centres to cover security services according to the number of employees per sector.

# 4.0 Effectiveness and Efficiency of Security Function Delivery within the Department

## 4.1 Security Function Administration

### 4.1.1 Education and Training on Security

There is no formal security awareness program for departmental employees. Awareness training is conducted on an "as requested" basis. The Intranet site of Human Resources Branch includes also a page dedicated to security which includes departmental security policies as well as information of common use about the services. The regions do not have any awareness programs, except that sometimes reminders are sent electronically to staff in the British Columbia and Quebec.

The background paper on the security function, which was prepared for a colloquium with the Industry Sector, has recently been reproduced on a large scale in order to try to implement a more proactive program. The officer of staff awareness also indicated that the documents should be customized for each sector and region to reflect distinct features. Auditors noticed that the content of this document pertains more to practical information about security services, rather than to developing awareness in the true sense of the term.

The SSD staff wants to have more time and budget for the training of employees related to the security function. The same problem was raised in the Quebec Region where the lack of security training adversely affects managers because of limited knowledge in the field. The representatives of the Quebec and Atlantic Regions also reported that central services provided little support for information and awareness services.

**Recommendation**

It is recommended that the Director, Compensation, Security and Management Services put in place a formal security awareness program, which would encompass regions as well as Headquarters.

### 4.1.2 Classification and Designation of Sensitive Information and Assets

Presently, three classification guides from the old departments constituting Industry Canada are being used for the classification and designation of information. However, a new guide for the Department is in process of being developed and should be available by the end of February 2000.

The audit with managers responsible for file rooms shows that classified and protected information is labelled with the required security markings (i.e., protected, secret or top secret). On the other hand, the Department does not assign the A, B, C ratings for protected documents, as is specified in the TB policy. At the same time, in the absence of a sole classification guide reflecting ongoing departmental activities, the manager in charge of records management for the NCR does not perform any controls to verify if some documents are over or under classified.

There are no procedures or controls in place to ensure that documents required to be declassified after a certain period of time are, in fact, declassified systematically, at the request of managers. This situations increases the risk of over classification, and creates a congestion in file rooms during peak periods. On the other hand, the Department's records retention and disposal schedule seems to be followed and is compatible with TB policy. In regions, security officers reported that they are not aware of all the procedures for records classification and protection.

**Recommendation**

The Director, Compensation, Security and Management Services should ensure that the Department's new classification guide is part of the awareness program, that it ensures a follow-up and that it prompts managers to advise file rooms when documents are declassified.

### 4.1.3 Threat and Risk Management Method

The preliminary audit revealed that there is no Department-wide method for threat and risk management. There is presently no documentation which describes risks by sector, by business type or by location, and which is based on one method of assessment. However, it was noted that the risks associated to the Department are well known by the SSD staff concerning the main buildings (such as C.D. Howe and Jean Edmond) and some other secondary locations.

The assessment of threats and risks is a central component in the risk management method. However, threat and risk assessments have not been conducted in Industry Canada buildings at Headquarters or in the regions since the creation of Industry Canada.. The SSD recently engaged a consultant to conduct such an assessment in the C.D. Howe building. According to the TB policy, this type of assessment - which in principle could be performed by departmental employees - should be conducted in all buildings where the frequency of reported incidents and infringements and where the nature of assets and information seem to justify it.

**Recommendation**

It is recommended that the Director, Compensation, Security and Management Services establish a priority list of buildings, including those in the Regions, for which the Director considers appropriate to conduct a threat and risk assessment and establish a timeline for these assessments.

### 4.1.4 Offense, Infringement and Other Security-Related Incidents

Auditors observed that there is a process within the Department to deal with cases of offense, infringement and other security-related incidents. When one of these cases is reported to the Security Services Division, a standard report is used to enter all relevant data.

A part of the information from reports is usually entered in a computer program "Lotus Approach". Entires have not been made since September 1999 due to technical problems. The SSD wants to modify this database in order to make it more compatible with their needs. Auditors noticed that this database is not presently used to analyse the overall incidents and infringements (types, locations, periods), although it represents an interesting tool to assess threats and risks.

In principle, all infringement and incident cases should be reported to the SSD. However, it was mentioned that some sectors or regions do not always report these cases because they do not want to call attention on their potential lack of efficient security measures. We observed that for the period of March 1996 to August 1999, on a total of 261 cases, only four incident or infringement cases came from regions. When asked to comment on these infringement and incident cases, regional officers did not provide any clear answers regarding the procedures to be followed and reported few known cases, but they admitted that there is no guarantee that all incidents and infringements have been reported.

There is an internal policy on infringements and incidents, but like all the other policies, it needs to be revised.

**Recommendations**

It is recommended that the Director, Compensation, Security and Management Services reinforce awareness efforts among regions to ensure that any type of infringement, offense or incident is reported to the SSD.

It is recommended that the Director, Compensation, Security and Management Services change the infringement and incident database so as to use it as an analysis tool in order to measure threats and risks associated to types of events, locations, period of year, etc.

## 4.2 Physical Security

### 4.2.1 Site and Accommodation of Facilities Enabling Risk Reduction or Elimination

Through our review of the Department's physical security, we observed that security requirements were, in general, taken into account during the choice of a site, the acquisition or the construction of a new accommodation, or a simple renovation. Facilities management services staff communicate to the SSD any new construction or new accommodation plans. The division then reviews these plans, makes recommendations and makes site visits at the end of the projects to ensure compatibility,

However, according to the SSD, regions do not follow this procedure. As the Quebec and Atlantic Regions reported the lack of security training and the lack of support from the head office (especially for aspects related to physical security), there is no evidence that all important criteria are taken into account during new construction or moves.

**Recommendation**

It is recommended that the Director, Compensation, Security and Management Services develop a list of steps to be followed as a control tool to help regional security coordinators and senior managers in ensuring that all significant security elements are considered during new construction or moves.

### 4.2.2 Physical Protection Measures

In the NCR, the Department has offices in 15 locations. The SSD offers these locations an array of services related to physical protection and emergency measures, including camera surveillance, guards, ID cards, electronic access control and patrols. Our visit to the security control centre located at the Jean Edmond building revealed that the Department was equipped with a modern system, including an integrated access system (Level) and a security information management system (ID cards).

Auditors found that physical protection measures are satisfactory for several departmental offices. However, some weaknesses were identified in ensuring this protection, especially in some secondary locations in the NCR and in the regions.

For the main buildings in which the Department occupies office space, we were told that most of the areas at risk, such as the file rooms and the computer control rooms, are well protected,. But the SSD could not ascertain whether measures are adequate for buildings where the Department has a low number of employees, especially since a security system audit has not been conducted. On the other hand, we observed that access to offices of the C.D. Howe building is well protected in the evening and during week-ends, but often open to public during regular work hours. According to the DSO, most of the reported infringements/incidents related to theft of personal belongings are the consequence of this open access. However, this weakness should be addressed in the threat and risk assessment being conducted for the C.D. Howe building.

According to the DSO, departmental employees are aware of the appropriate measures to protect classified and protected documents. However, there are no security "sweeps" (control measures) undertaken outside regular work hours to verify if employees have placed documents in locked cabinets. This might increase the possible access of classified or protected documents by employees who do not have the corresponding security ratings or by the public in the case of C.D. Howe building.

Interviewees noted that there is no guarantee that regional offices have all the necessary physical protection measures, both for assets and employees. The SSD believes that there are gaps in several areas, such as easy access to work space from the reception area.

Finally, the audit indicated that since the creation of Industry Canada, the SSD has inspected some departmental offices in the NCR. In the case of regions, only the regional administration offices of Place Ville-Marie in Montreal have been subject to an audit of physical security by the SSD, after which remedial actions were brought by the regional officer. In the Atlantic Region, advisory meetings were also held by the SSD. However, we observed that there is no periodic review or control program of physical security measures for all of the locations of Industry Canada.

**Recommendations**

Given the uncertainty related to the absence of controls performed outside regular work hours (sweeps) to verify if employees have placed documents in locked cabinets, it is recommended that the Director, Compensation, Security and Management Services ensure that this gap is addressed in the threat and risk assessment for C.D. Howe building.

Given the uncertainty with regard to physical protection measures in regional offices, it is recommended that the Director, Compensation, Security and Management Services inform all regions of the measures to take to ensure a physical security in their offices, and conducts a follow-up.

It is recommended that the Director, Compensation, Security and Management Services establish a periodic review and control program of physical security measures for all the locations occupied by the Department.

## 4.3 Personnel Security

The SSD is responsible for the administration of security and reliability rating of all employees reporting to Industry Canada's Deputy Minister. The Department's policy is to require, at a minimum, an enhanced level of reliability as soon as a permanent employee or a term employee has access to Industry Canada's offices.

The audit found that the Department has a security investigation program which is relatively compatible with the government security policy and with the personnel security standard. The interview with the manager in charge of security revealed the existence of a clear and well-established process, both for offices in the NCR and in the regions. The regions must, in fact, use the security investigation service offered by Headquarters.

The SSD conducts periodic audits of sample of files for personnel security. These audits verify, for example, if signatures of individuals have been obtained for their consent to be subject to an investigation, if dates show that the individual began work after the result of the investigation, etc. However, we observed that, despite these audits and the awareness efforts, including a guide made available to managers, there are still some weaknesses:

- The government security policy stipulates that a permanent employee or a term employee should hold office only once the result of the security/reliability investigation is obtained. The manager of personnel security indicated that this condition is generally respected in the case of permanent positions, but a contract worker or a trainee often has access to the departmental offices without knowing the result of the inquiry or, even worse, without initiating an inquiry request. Awareness campaigns for managers in the NCR and in some regions have helped to improve the situation, but there is still room for improvement according to the manager. In the Quebec Region, auditors were told that to offset this trend, regional informatics services will henceforth give a computer access account only when an employee receives the result of his or her security inquiry, as prescribed by the Treasury Board's informatics security policy.

- The government security policy requires that the security/reliability ratings be updated every ten years, except for the very secret level which must be updated every five years. According to the manager of personnel security services, the update of security ratings can extend up to eleven years.

With regard to the disposal of security files, the SSD mentioned that this is done in compliance with the records retention and disposal schedule of National Archives of Canada.

**Recommendations**

It is recommended that the Director, Compensation, Security and Management Services enhance the awareness among managers, including regional managers, in order to avoid that contract workers and trainees having access to the departmental offices or beginning to work before obtaining their security/reliability ratings.

It is recommended that the Director, Compensation, Security and Management Services ensure that the period of updating security/reliability ratings is compliant with Treasury Board recommended level.

## 4.4 Security and Management of Emergencies

The audit showed that necessary measures have been followed to protect sensitive information and assets, as well as employees, during any type of emergency, for all the locations where the Department has many employees. Procedures are available for both security staff and employees. For locations where the Department occupies a small portion of the available space, the SSD reports that they have assessed the measures taken by the owners or the main tenants of the buildings and that these measures are compatible with Treasury Board's policy.

# 5.0 Conclusion

This preliminary audit demonstrated that, despite a few weaknesses identified, the security function within the NCR does not present any major problems, especially for the key locations.

The most important recommendations refer to the organization and administration of security function. Since these recommendations will prompt the SSD to take many significants actions in the Department's locations in the NCR and in the regions, it would not be advisable, at this point, to conduct a further audit of security function. However, it would be appropriate to conduct a follow-up of the status of implementation of recommendations in one to two years time. This follow-up could include a visit to one or two regional offices, if deemed appropriate.

Industrie Canada Industry Canada

# Vérification de la fonction sécurité
# Rapport de phase préliminaire

**Direction générale de la vérification et de l'évaluation**

**Janvier 2000**

Canada

# TABLE DES MATIÈRES


**1.0 Objectifs de la vérification ..... 1**

**2.0 Étendue et approche de la vérification ..... 1**

**3.0 Cadre de gestion de la fonction sécurité ..... 2**

3.1 Organisation de la sécurité ..... 2

3.2 Plan et politique de sécurité ..... 3

3.3 Recouvrement de coûts pour les services de sécurité ..... 4

**4.0 Efficacité et efficience de la mise-en-oeuvre de la fonction de sécurité au sein du Ministère ..... 6**

4.1 Administration de la fonction sécurité ..... 6

4.1.1 Éducation et formation en matière de sécurité ..... 6

4.1.2 Classification et désignation des renseignements et des biens de nature délicate ..... 6

4.1.3 Méthode de gestion des menaces et risques ..... 7

4.1.4 Infractions, violations et autres incidents relatifs à la sécurité ..... 8

4.2 Sécurité matérielle ..... 8

4.2.1 Site et aménagement des installations permettant la réduction ou l'élimination des risques ..... 8

4.2.2 Mesures de protection matérielle ..... 9

4.3 Sécurité du personnel ..... 10

4.4 Sécurité et gestion des cas d'urgence ..... 12

**5.0 Conclusion ..... 13**

## 1.0 Objectifs de la vérification

Le but de la phase préliminaire est d'évaluer l'efficacité de la fonction sécurité d'Industrie Canada et d'identifier les aspects clés de cette fonction qui devraient faire l'objet d'une vérification plus approfondie.

Les objectifs de la phase préliminaire étaient les suivants:

- Évaluer le cadre de gestion utilisé par la Division des services de sécurité (DSS), incluant l'efficacité de la politique sur la sécurité du Ministère et son niveau de conformité avec la politique sur la sécurité du Conseil du Trésor;
- Évaluer l'efficacité et l'efficience de la mise-en-oeuvre de la fonction de sécurité au sein du Ministère.

## 2.0 Étendue et approche de la vérification

La phase préliminaire a couvert tous les secteurs du Ministère, incluant une évaluation sommaire de la sécurité pour les régions du Pacifique/Yukon, du Québec et des Maritimes par l'entremise d'entrevues téléphoniques. Les éléments suivants ont été vérifiés:

- Organisation de la sécurité;
- Administration de la sécurité;
- Sécurité matérielle;
- Sécurité du personnel;
- Sécurité et gestion des cas d'urgence;
- Sécurité et gestion des marchés.

L'élément sécurité de l'information technologique, qui fait partie maintenant du Bureau principal de l'information, a été exclu de cette vérification en raison de son caractère distinct. Cependant le lien fonctionnel entre le responsable de la sécurité informatique et la DSS a été évalué.

Nous avons effectué 15 entrevues avec les gestionnaires et les employés liés à la fonction sécurité. Le guide de vérification de la sécurité du Conseil du Trésor (juillet 1996) a été utilisé comme outil de référence lors des entrevues et de la revue de la documentation pertinente.

# 3.0 Cadre de gestion de la fonction sécurité

## 3.1 Organisation de la sécurité

La responsabilité d'assurer la sécurité dans le Ministère revient à tous les gestionnaires alors que la Division des services de sécurité est responsable de la gestion des divers éléments reliés à celle-ci.

La Division des services de sécurité (DSS) relève la Directrice, rémunération, sécurité et services de gestion de la Direction générale des ressources humaines. Elle compte sept employés à temps plein, 27 employés engagés à contrat avec le corps des commissionnaires et un avec Pinkerton.

Le directeur de gestion de la DSS est l'agent de sécurité du Ministère (ASM), lequel a le mandat d'élaborer, de mettre en oeuvre, de maintenir, de coordonner et de contrôler le programme de sécurité d'Industrie Canada. L'ASM a un rôle hiérarchique avec la plupart des secteurs du Ministère, sauf dans le cas du Conseil canadien de la recherche (CCR) et de l'Office de la propriété intellectuelle du Canada (OPIC) et Mesures Canada, pour lesquels il a un rôle fonctionnel.

L'ASM est secondé par trois gestionnaires dont un pour la sécurité du personnel, un pour la sécurité matérielle et la planification des mesures d'urgence, et un pour la gestion du recouvrement des coûts et la sensibilisation à la sécurité. La fonction de la sécurité de l'information technologique relève du Bureau principal de l'information depuis le début d'octobre 1999. Selon le gestionnaire responsable de cette fonction, ce transfert n'a provoqué aucun changement négatif pour la DSS puisqu'il doit tenir l'ASM informé de toute information importante reliée à la sécurité de l'information. La Direction des ressources humaines est sur le point de revoir la description de tâche de l'ASM suite à ce transfert.

L'ASM joue un rôle fonctionnel vis-à-vis les régions. Dans tous les bureaux régionaux, des responsables ont été nommés pour la sécurité du personnel et pour la sécurité matérielle et la planification des cas d'urgence. Ces derniers ont la responsabilité d'appliquer des mesures de sécurité adéquates mais doivent partager le temps affecté à la sécurité avec d'autres tâches administratives.

Lors de la phase préliminaire, la DSS nous a indiqué que le poste de l'agent responsable pour le système intégré électronique de contrôle d'accès et de système d'identification qui est présentement occupé par un contractuel est en voie d'être doté. Cette dotation permettra d'assurer la continuité de ce service.

Lors de la phase préliminaire, l'équipe de vérification a constaté que tous les éléments de la fonction sécurité sont couverts par les postes de la DSS. Cependant, ils ont observé les faiblesses suivantes dans l'organisation de la sécurité pour le Ministère:

- La DSS offre des services à des organisations externes dont les plus importants sont Citoyenneté et Immigration Canada (CIC) et le Bureau du vérificateur général.

L'acquisition par le Ministère du centre de contrôle situé à l'édifice Jean Edmond explique en partie cette situation. Or, il est difficile de trouver une justification valable à cet état de faits, compte tenu qu'un niveau de sécurité accru est nécessaire pour les opérations de CIC et que le Ministère n'est pas le principal locataire de cet édifice.

- Certains responsables régionaux ne pouvaient donner avec précision leur rôle et leur définition de tâches en matière de sécurité. D'autre part, l'insuffisance de personnel et de fonds a été invoquée par l'ASM pour expliquer le manque d'implication de sa Division dans les régions, en particulier pour le suivi des mesures de sécurité.

D'autre part, la DSS semble entretenir des liens étroits avec les fonctions santé et sécurité au travail, gestion immobilière et matérielle, et dotation. En ce qui regarde l'importance des liens externes avec des organismes tels que la GRC (sécurité matérielle) et TPSGC (sécurité relative aux marchés), ils nous ont semblé satisfaisants.

**Recommandation**

Il est recommandé que la Directrice, rémunération, sécurité et services de gestion analyse la pertinence d'offrir des services de sécurité (et autres) à d'autres organismes gouvernementaux. Cet examen pourrait inclure une analyse comparative avec les services communs de sécurité pour d'autres édifices gouvernementaux occupés par différents ministères.

## 3.2 Plan et politique de sécurité

Notre analyse préliminaire a permis de constater que le Ministère n'a pas de plan de sécurité formel en place. Bien que plusieurs initiatives futures aient été présentées par le personnel de la DSS, il ne semble pas que celles-ci s'insèrent dans un plan détaillé contenant des buts et objectifs à court, moyen et long terme. De plus, les activités des régions en matière de sécurité sont exclues. Ce plan devrait également être intégré au plan stratégique du Ministère et approuvé par la haute gestion. L'ASM nous a indiqué que des efforts sont faits afin de convaincre la haute gestion vis-à-vis l'établissement d'un plan sur la sécurité pour tout le Ministère.

Les entrevues avec les responsables de la sécurité dans les bureaux régionaux ont révélé que certaines régions n'ont pas de processus de planification ou de programme pour la sécurité. Alors que la région du Pacifique/Yukon semble plus pro-active dans l'application de mesures diverses et dans la gestion d'ensemble de la sécurité pour leurs bureaux, les régions des Maritimes et du Québec ont une approche plutôt réactive.

Nous avons également constaté que le Ministère ne possède pas de politique globale pour la sécurité. Il existe d'anciennes politiques provenant des ministères qui ont fait partie de l'amalgamation menant à la formation d'Industrie Canada. Ces politiques sont accessibles sur le site Intranet de la Direction générale des ressources humaines. Cependant, ces politiques devront être révisées afin d'enlever les références aux anciens ministères et de tenir compte de la révision de la politique sur la sécurité du gouvernement (PSG) qui a été réalisée en 1994. Il ne semble pas exister d'agenda formel pour la révision des ces politiques ou pour le développement d'une politique globale sur la sécurité au Ministère.

**Recommandations**

La Directrice, rémunération, sécurité et services de gestion devrait élaborer un programme de sécurité complet, c'est-à-dire un plan qui inclut tous les éléments de la fonction sécurité, tous les secteurs du Ministère et toutes les régions.

La Directrice, rémunération, sécurité et services de gestion devrait élaborer et mettre en oeuvre un plan visant à créer une politique globale sur la sécurité pour le Ministère ou mettre à jour les politiques existantes.

## 3.3 Recouvrement de coûts pour les services de sécurité

La responsabilité pour le recouvrement des coûts des services de sécurité relève du Directeur de gestion de la DSS. La facturation et le recouvrement des fonds sont effectués par l'Agent administratif des services administratifs de la Direction générale des ressources humaines (DGRH).

Il existe deux types de recouvrements de coûts, 1) les services fournis aux autres ministères et agences gouvernementales et 2) les services à l'intérieur du ministère.

**Services aux autres ministères et agences gouvernementales**

Le Ministère a présentement des ententes de service avec cinq organismes, soit le Bureau du Canada pour le Millénaire; Citoyenneté et immigration Canada; l'Office de la propriété intellectuelle du Canada; le Conseil canadien des relations industrielles; et la Commission des relations de travail dans la fonction publique. Il s'agit d'ententes d'une durée de un à trois ans avec clause de renouvellement automatique. Chaque entente est un peu différente car elle comporte des niveaux de service couvrant une partie de la fonction de sécurité à l'ensemble des services corporatifs.

Les termes de recouvrement sont différents d'une entente à l'autre. Ils varient d'un taux par service (carte d'identité, accès etc.) à un partage des frais (Corps des Commissionnaires). La facturation est effectuée à tous les trimestres par l'agent administratif des services administratifs de la DGRH.

Nous avons également constaté que le Ministère fourni des services à d'autres organismes sans qu'il n'y ait d'entente formelle, soit le Bureau du vérificateur général du Canada (cartes d'identités, sécurité du personnel, bureau d'information, service de base de l'immeuble); Développement des ressources humaines Canada (système d'urgence) et l'Agence spatiale canadienne (système d'urgence).

Notre analyse préliminaire a révélé que la base servant de calcul pour la facturation est inadéquate. Aucune analyse de coûts n'a été effectuée pour déterminer les coûts réels et complets pour les taux des services offerts et pour le partage des coûts. Les coûts sont présentement basés sur des estimés et aucune analyse annuelle n'est effectuée pour majorer les coûts selon

l'augmentation des dépenses encourues. En plus nous avons constaté que le partage des coûts pour les commissionnaires n'inclut pas les frais généraux (supervision, etc.)

**Services à l'intérieur du Ministère**

Les mêmes services sont offerts à l'intérieur du Ministère sur une base de recouvrement des coûts depuis 1995. Cette approche a été mise en place pour palier à un manque de ressources au sein de la DGRH. La DSS a présentement un budget de 337 000$ pour les salaires, et 66 000$ pour ses dépenses d'opérations. En plus elle reçoit un transfert budgétaire de 400 000$ du Bureau du sous-ministre pour le Corps des commissionnaires. Le recouvrement des coûts apporte un supplément d'environ 1.2M$ à la DSS.

L'activité de recouvrement des coûts présente quelques problèmes pour l'organisation. Premièrement, la sécurité au Ministère est une fonction essentielle, et les employés de la DSS et de la DGRH nous ont indiqué que cela ajoute du travail pour le maintien d'un système de facturation. En plus nous avons constaté que:

- La facturation pour chaque carte d'identité et chaque demande de modification aux accès a pour effet de décourager les centres de responsabilité à demander le service et créer une situation ou l'on demande des périodes plus longues et plus risquées dans le seul but de minimiser les coûts;
- Selon les entrevues, il est possible que certains gestionnaires évitent de faire exécuter des vérifications de sécurité sur les employés temporaires et sur les consultants afin d'éviter les coûts qui y sont rattachés;
- La facturation du temps des employés de la DSS a pour effet de transférer des dépenses d'opérations d'un centre de responsabilité pour couvrir des dépenses de salaire de la DSS. Ces transferts entre les dépenses d'opération et les salaires faussent le rapport des dépenses au sein du Ministère.

En conclusion, le recouvrement des coûts est nécessaire pour les services offerts aux autres organismes à l'extérieur du Ministère. Toutefois il est indispensable d'avoir un système adéquat qui permet d'avoir les coûts réels et complets. En ce qui concerne le recouvrement interne, cela semble ni plus ni moins être une méthode compliquée pour un simple transfert de budget entre centres de responsabilité.

**Recommandations**

La Directrice, rémunération, sécurité et services de gestion devrait développer un système pour évaluer les coûts réels reliés aux opérations de la DSS et devrait réviser ces taux sur une base annuelle.

La Directrice, rémunération, sécurité et services de gestion devrait revoir sa politique de facturation à l'interne et utiliser l'information découlant de l'évaluation des coûts réels afin d'établir, au début de chaque année, un transfert budgétaire à partir des autres centres de responsabilité pour couvrir les services de sécurité au prorata du nombre d'employés par secteur.

# 4.0 Efficacité et efficience de la mise-en-oeuvre de la fonction de sécurité au sein du Ministère

## 4.1 Administration de la fonction sécurité

### 4.1.1 Éducation et formation en matière de sécurité

La DSS n'a pas de programme formel pour la sensibilisation à la sécurité auprès des employés du Ministère. La sensibilisation se fait présentement sur demande seulement. Il existe également une page pour la sécurité sur le site Intranet de la Direction générale des ressources humaines dans laquelle on retrouve les politiques de Ministère en matière de sécurité ainsi que de l'information d'usage courant concernant les services. Dans les régions, il n'y a pas de programme de sensibilisation mis-à-part les rappels aux employés par voie électronique qui se font couramment dans la région de la Colombie-Britannique et quelquefois dans la région du Québec.

Le document d'information sur la fonction de sécurité qui a été préparé pour la journée d'information avec le secteur Industrie vient tout juste d'être reproduit en grande quantité pour d'autres expériences du même genre et pour tenter de mettre en place un programme plus pro-actif. Le responsable de la sensibilisation aux employés a également indiqué que les documents devraient être adaptés aux secteurs et aux régions afin de tenir compte de la spécificité de chacun. Nous avons constaté que le contenu de ce document s'apparente davantage à de l'information pratique concernant les services de sécurité que de la sensibilisation proprement dite.

À la DSS, on souhaiterait avoir davantage de temps et de budget pour la formation des employés liés à la fonction de la sécurité. Le même problème a été soulevé dans la région du Québec où le manque de formation en sécurité nuit à la gestion en raison des connaissances restreintes. Il a également été indiqué par les représentants des régions du Québec et des Maritimes que le soutien en service d'information et de sensibilisation de la part des services centraux est pratiquement inexistant.

**Recommandation**

Il est recommandé que la Directrice, rémunération, sécurité et services de gestion mette en place un programme formel de sensibilisation à la sécurité, lequel devrait inclure les régions.

### 4.1.2 Classification et désignation des renseignements et des biens de nature délicate

Présentement, trois anciens guides de classification provenant d'anciens ministères faisant partie maintenant d'Industrie Canada sont utilisés pour la classification et la désignation des renseignements. Cependant un nouveau guide s'adressant à tout le ministère est sur le point d'être élaboré et devrait être disponible à la fin de février 2000.

La vérification auprès du gestionnaire responsable des salles de dossiers a permis de constater que les renseignements classifiés et protégés portent les mentions de sécurité requises, soit protégé, secret ou très secret. Par contre, le Ministère n'attribue pas les cotes A,B et C pour les documents protégés, comme il est spécifié dans la politique du CT. D'autre part, en l'absence

d'un guide de classification unique qui tient compte des activités courantes du Ministère, le gestionnaire responsable de la gestion des dossiers pour la RCN ne fait aucun contrôle pour vérifier si certains documents sont sur ou sous classifiés.

Il n'existe pas de procédure ni de contrôle pour s'assurer que les documents dans les salles de dossier qui devraient être dé-classifiés après un certain temps le sont de façon systématique à la demande des gestionnaires. Cette situation augmente le risque de sur-classification des documents en plus de créer un engorgement des salles de dossiers en période de pointe. Par contre, le plan de conservation et d'élimination des documents du Ministère semble bien suivi et en conformité avec la politique du CT. Dans les régions, les responsables de la sécurité nous ont révélé qu'ils ne sont pas au courant de toutes les procédures de classification et de protection des documents.

**Recommandation**

La Directrice, rémunération, sécurité et services de gestion devrait s'assurer que le nouveau guide de classification du Ministère fasse partie du programme de sensibilisation, en assure le suivi et incite les gestionnaires à aviser la salle des dossiers lorsqu'un de leurs documents est dé-classifié.

### 4.1.3 Méthode de gestion des menaces et risques

Notre vérification préliminaire a permis de constater qu'il n'existe pas de méthode de gestion des menaces et risques pour l'ensemble du Ministère. Il n'y a présentement aucune documentation qui décrit les risques par secteur, par type d'activité ou par emplacement et qui fait état d'une méthode. Cependant, nous avons remarqué que les risques associés aux activités du Ministère sont bien connus par le personnel de la DSS en ce qui concerne les principaux édifices tels que le C.D. Howe et le Jean Edmond, et pour certains autres emplacements secondaires.

L'évaluation des menaces et des risques est un élément central dans une méthode de gestion des risques. Or, le Ministère n'a fait aucune évaluation des menaces et des risques dans ses établissements depuis la formation d'Industrie Canada, autant à l'administration centrale que dans les régions. Cependant, la DSS vient d'engager un consultant pour effectuer une telle évaluation à l'édifice C.D. Howe. Ce type d'évaluation, qui en principe peut être effectuée par les employés du Ministère, devrait, selon la politique du CT, être effectuée dans tous les établissements où la fréquence des incidents et violations qui sont rapportés et où la nature des biens et des renseignements semblent le justifier.

**Recommandation**

Il est recommandé que la Directrice, rémunération, sécurité et services de gestion établisse une liste de priorité des établissements, incluant ceux des régions, pour lesquels elle juge appropriée d'effectuer une évaluation des menaces et des risques et établir un échéancier pour ces évaluations.

### 4.1.4 Infractions, violations et autres incidents relatifs à la sécurité

Nous avons constaté qu'il existe au Ministère un processus pour traiter des cas d'infractions, de violations et d'autres incidents relatifs à la sécurité. Lorsqu'un de ces cas est rapporté à la Division des services de sécurité, on utilise un rapport standard pour y entrer toutes les données pertinentes.

Une partie des informations provenant des rapports est normalement entrée dans un programme informatisé "Lotus Approach", ce qui n'a pas été fait depuis septembre 1999 en raison de problèmes techniques. La DSS souhaite modifier cette base de données de façon à la rendre plus compatible avec leurs besoins. Nous avons constaté que cette base de donnée n'est présentement pas utilisée pour analyser l'ensemble des incidents et infractions (types, lieux, périodes), alors qu'elle constitue un outil intéressant pour évaluer les menaces et les risques.

En principe, tous les cas d'infractions et d'incidents devraient être rapportés à la DSS. Cependant, il nous a été mentionné que certains secteurs ou régions ne le font pas toujours afin de ne pas trop attirer l'attention sur le manque possible de mesures de sécurité efficaces. Nous avons remarqué que seulement quatre cas d'incidents ou d'infractions sur un total de 261 pour la période de mars 1996 à août 1999 provenaient des régions. Lorsqu'appelés à commenter les cas d'infractions et d'incidents, les responsables régionaux étaient vagues quant aux procédures à suivre et ont rapporté peu de cas connus, mais ils avouent qu'il n'existe aucune assurance que tous les incidents et infractions sont rapportés.

Il existe une politique interne pour les infractions et incidents, mais celle-ci comme toutes les autres politiques, doit faire l'objet d'une révision.

**Recommandations**

Il est recommandé que la Directrice, rémunération, sécurité et services de gestion accentue les efforts de sensibilisation auprès des régions afin de s'assurer que tout type d'infraction, de violation ou d'incident soit rapporté à la DSS.

Il est recommandé que la Directrice, rémunération, sécurité et services de gestion modifie la base de données des infractions et incidents de façon à l'utiliser comme un outil d'analyse permettant de mesurer les menaces et risques associés aux types d'événements, aux lieux, à la période de l'année, etc.

## 4.2 Sécurité matérielle

### 4.2.1 Site et aménagement des installations permettant la réduction ou l'élimination des risques

Notre examen de la sécurité matérielle du Ministère a permis de constater que les exigences de sécurité sont, en général, prises en compte dans le choix d'un site, dans l'acquisition ou la construction d'un nouvel aménagement ou lors d'une simple rénovation. Les services de la gestion des installations communiquent à la DSS tous les plans de nouvelles constructions ou de

nouveaux aménagements. Cette dernière étudie les plans, émet des recommandations et effectue des visites à la fin des projets pour s'assurer que tout est conforme.

Dans les régions cependant, cette façon de faire n'est pas suivie selon la DSS. Comme les régions du Québec et des Maritimes ont mentionné le manque de formation en sécurité ainsi que le manque de soutien de la part du bureau chef, spécialement pour les aspects liés à la sécurité matérielle, rien n'indique que tous les critères importants sont pris en considération lors des nouvelles constructions ou aménagements.

**Recommandation**

Il est recommandé que la Directrice, rémunération, sécurité et services de gestion élabore une liste d'étapes à suivre comme outil de contrôle qui permettrait aux coordonnateurs de la sécurité et aux principaux gestionnaires dans les régions de s'assurer que tous les éléments de sécurité importants soient pris en compte lors de nouvelles constructions ou de nouveaux aménagements.

### 4.2.2 Mesures de protection matérielle

Dans la RCN, on dénombre quinze emplacements où le Ministère a des bureaux. La DSS fournit à ces emplacements une panoplie de services liés à la protection matérielle et aux mesures d'urgence incluant, entre autre, la surveillance par caméra, des gardiens, les cartes d'identité, le contrôle d'accès électronique et des patrouilles. La visite du centre de contrôle de sécurité situé à l'édifice Jean Edmond a permis de constater que le Ministère s'est doté d'un système moderne, incluant un système d'accès intégré (Lenel) et d'un système de gestion de l'information de sécurité (cartes d'identité).

Notre vérification a permis de constater que les mesures de protection matérielle sont satisfaisantes pour plusieurs bureaux du Ministère. Cependant certaines faiblesses ont été remarquées quant au processus visant à assurer cette protection, spécialement à certains emplacements secondaires de la RCN et dans les régions.

Pour les principaux édifices où le Ministère occupe des bureaux, il nous a été mentionné que la plupart des endroits à risques, tels que les salles de dossiers et salles de contrôle informatique, sont très bien protégés. Mais la DSS ne peut affirmer que les mesures sont adéquates aux édifices où le Ministère compte un faible nombre d'employés, spécialement lorsque la vérification du système de sécurité n'a pas été réalisée. D'autre part, nous avons observé que l'accès aux bureaux de l'édifice C.D. Howe est bien protégé le soir et les fins de semaine, mais ouvert au public lors des heures de bureau. Selon l'ASM, la majorité des infractions/incidents reliés à des vols d'effets personnels qui ont été rapportés sont la conséquence de ce libre-accès. Cependant, cette faiblesse devrait être normalement prise en compte dans l'évaluation des menaces et des risques qui est effectuée présentement pour l'édifice C.D. Howe.

Selon l'ASM, les employés du Ministère savent quelles sont les mesures appropriées pour protéger les documents classifiés et protégés. Cependant, les contrôles qui permettaient de vérifier hors des heures de bureau (sweeps) si les employés plaçaient les documents dans les

cabinets barrés ne se font plus. Ce changement risque d'augmenter la possibilité que des documents classifiés ou protégés soient accessibles par des employés qui n'ont pas la cote sécuritaire correspondante ou par le public dans le cas de l'édifice C.D. Howe.

Les entrevues ont démontré qu'il n'est pas assuré que les bureaux régionaux ont toutes les mesures de protection matérielles nécessaires, autant pour les biens que pour les employés. La DSS croit que plusieurs lacunes existent à plusieurs endroits, tel que l'accès trop facile à la zone de travail à partir de la zone de réception.

Enfin, notre vérification indique que depuis la formation d'Industrie Canada, la DSS a effectué des inspections de quelques bureaux du Ministère dans la RCN. Pour les régions, seuls les bureaux de l'administration régionale de la Place Ville-Marie à Montréal ont fait l'objet d'une vérification de la sécurité matérielle par la DSS, à la suite de laquelle les correctifs ont été apportés selon la responsable régionale. Dans la région des Maritimes, des rencontres de consultation ont également été menées par la DSS. Cependant, nous avons constaté qu'il n'existe pas de programme d'examen et de contrôle périodique des mesures de sécurité matérielle pour l'ensemble des emplacements d'Industrie Canada.

**Recommandations**

Étant donné l'incertitude liée à l'arrêt des contrôles qui permettaient de vérifier hors des heures de bureau (sweeps) si les employés placent les documents dans les cabinets barrés, il est recommandé que la Directrice, rénumération, sécurité et services de gestion s'assure que cette lacune fasse partie de l'évaluation des menaces et des risques pour l'édifice C.D. Howe.

Étant donné l'incertitude quant aux mesures de protection matérielle dans les bureaux régionaux, il est recommandé que la Directrice, rémunération, sécurité et services de gestion informe les régions des mesures à prendre pour assurer la sécurité matérielle dans leurs bureaux et effectue un suivi.

Il est recommandé que la Directrice, rémunération, sécurité et services de gestion établisse un programme d'examen et de contrôle périodique des mesures de sécurité matérielle pour tous les emplacements occupés par le Ministère.

## 4.3 Sécurité du personnel

La DSS est responsable de l'administration des cotes sécuritaires et de fiabilité de tous les employés qui relèvent du Sous-ministre d'Industrie Canada. Le Ministère a comme politique d'exiger au minimum une cote de fiabilité approfondie dès qu'un employé permanent ou à terme a accès aux bureaux d'Industrie Canada.

Notre vérification a démontré qu'il existe un programme d'enquête de sécurité au sein du Ministère qui est relativement conforme à la politique sur la sécurité du gouvernement et à la norme sur la sécurité du personnel. L'entrevue avec le gestionnaire responsable de la sécurité a démontré l'existence d'un processus clair et bien établi, autant pour les bureaux de la RCN que

pour ceux des régions. Ces derniers doivent en effet utiliser le service d'enquête de sécurité offert par l'administration centrale.

La DSS effectue périodiquement des vérifications d'un échantillon de dossiers pour la sécurité du personnel dans lesquels on vérifie, par exemple, si les signatures des individus ont été obtenues pour leur consentement à un type d'enquête donné, si les dates démontrent que l'individu est entré en fonction qu'après le résultat de l'enquête, etc. Cependant, nous avons observé que malgré ces vérifications et les efforts de sensibilisation qui sont déployés, lesquels incluent un guide mis à la disposition des gestionnaires, certaines lacunes subsistent:

- La politique de sécurité du gouvernement stipule qu'un employé permanent ou à terme ne devrait occuper sa fonction que lorsque le résultat de l'enquête de sécurité/fiabilité a été obtenu. Le gestionnaire de la sécurité du personnel a indiqué que cette condition est en général respectée dans le cas des postes permanents, mais qu'il arrive souvent qu'un employé contractuel ou qu'un stagiaire ait accès aux bureaux du Ministère sans que le résultat de l'enquête ne soit connu ou pire encore, sans qu'une demande d'enquête n'ait été initiée par le gestionnaire responsable. Des campagnes de sensibilisation auprès des gestionnaires de la RCN et de certaines régions ont permis d'améliorer la situation, mais il reste encore place à l'amélioration selon le gestionnaire. À la région du Québec, on a indiqué que pour contrer cette tendance, les services informatiques de la région vont dorénavant donner un compte d'accès informatique que lorsqu'un employé aura reçu le résultat de son enquête de sécurité, tel que prescrit par la politique de la sécurité informatique du Conseil du Trésor.
- La politique de la sécurité du gouvernement exige que les cotes de sécurité/fiabilité doivent être mises à jour à tous les dix ans, sauf pour le niveau très secret dont la fréquence est à tous les cinq ans. Selon le gestionnaire des services de sécurité du personnel, la mise à jour des cotes sécuritaires peut s'extensionner jusqu'à onze ans.

En ce qui concerne la destruction des dossiers de sécurité, la DSS a mentionné que le tout se fait en conformité avec le calendrier de conservation et d'élimination des Archives Nationales du Canada.

**Recommandations**

Il est recommandé que la Directrice, rémunération, sécurité et services de gestion accentue la sensibilisation auprès des gestionnaires, incluant ceux des régions, afin d'éviter que des employés contractuels et stagiaires aient accès aux bureaux du Ministère ou commencent à travailler avant que leur cote sécuritaire/de fiabilité ne soit obtenue.

Il est recommandé que la Directrice, rémunération, sécurité et services de gestion s'assure que la période à laquelle les cotes sécuritaires/de fiabilité sont mises à jour soit conforme au niveau recommandé par le Conseil du Trésor.

## 4.4 Sécurité et gestion des cas d'urgence

Notre vérification a permis de constater que les mesures nécessaires pour protéger les renseignements et les biens de nature délicate, de même que les employés, pendant tous les genres de cas d'urgence ont été prises pour tous les emplacements où le Ministère compte beaucoup d'employés. Des procédures sont disponibles autant pour le personnel de la sécurité que pour les employés. Pour les emplacements où le Ministère occupe une petite partie de la surface disponible, la DSS dit avoir évalué les mesures prises par les propriétaires ou principaux locataires des bâtiments et que celles-ci sont conformes à la politique du Conseil du Trésor.

# 5.0 Conclusion

Cette vérification préliminaire a permis de constater que malgré les quelques faiblesses qui ont été identifiées, la fonction sécurité dans la RCN ne pose pas de problèmes majeurs, spécialement pour les principaux emplacements.

Les recommandations les plus importantes ont trait à l'organisation et à l'administration de la fonction sécurité. Comme ces recommandations amèneront la DSS à entreprendre plusieurs actions importantes dans les emplacements du Ministère de la RCN et des régions, il ne serait pas utile, à ce stade, d'effectuer une vérification plus approfondie de la fonction sécurité. Cependant, il serait approprié d'effectuer un suivi des recommandations dans un an ou deux. Ce suivi pourrait inclure une visite dans un ou deux bureaux régionaux, si jugé approprié.